Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Qualifizierte DDoS-Mitigation Dienstleister

im Sinne § 3 BSIG

Stand: 19.Mai 2025

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0
E-Mail: qdl@bsi.bund.de
Internet: https://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2025

Inhalt

1 Hintergrund ... 4
2 Verfahren ... 5
3 Qualifizierte DDoS-Mitigation-Dienstleister ... 6
3.1 Akamai Technologies GmbH ... 6
3.2 Amazon Web Services ... 6
3.3 Babiel GmbH ... 6
3.4 Cloudflare GmbH ... 6
3.5 Colt Group ... 6
3.6 Corero Network Security ... 6
3.7 Deutsche Telekom AG ... 7
3.8 EWE ... 7
3.9 F5 Networks ... 7
3.10 Imperva Inc. ... 7
3.11 Inter.link GmbH ... 7
3.12 Link11 ... 7
3.13 M-net Telekommunikations GmbH ... 8
3.14 Myra Security GmbH ... 8
3.15 NaWas by NBIP ... 8
3.16 Netscout ... 8
3.17 noris network AG ... 8
3.18 Plus.line AG ... 8
3.19 Radware GmbH ... 8
3.20 Verizon Deutschland GmbH ... 9
3.21 Vodafone GmbH ... 9
3.22 Voxility ... 9
3.23 WEDOS GmbH ... 9
4 Leistungsmerkmale ... 10
4.1 Dienstangebot ... 10
4.2 Allgemeines zum Dienstleister ... 10
4.3 Angriff ... 11
4.4 Filtermöglichkeiten ... 11
5 Gegenüberstellung der Leistungsmerkmale der einzelnen DDoS-Mitigation-Dienstleister ... 13

1 Hintergrund

Das BSI hat gemäß § 3 BSIG die Aufgabe, Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik zu beraten und zu unterstützen. Hierzu kann auch auf qualifizierte Sicherheitsdienstleister verwiesen werden.

Angriffe auf Unternehmen nehmen in der letzten Zeit stark zu, sowohl in der Anzahl, als auch in der Intensität der Bedrohungen. Der Schaden, welcher dabei entsteht, verursacht bei den betroffenen Unternehmen nicht nur große wirtschaftliche Schäden, sondern auch einen Reputationsverlust, wenn Dienste nicht zur Verfügung stehen oder ein Datenabfluss zu verzeichnen war. Zur Verbesserung der Abwehr oder zur Bewältigung eines erfolgreichen Angriffs bedarf es vielfältig der Unterstützung externer Dienstleister, die in ihrem jeweiligen Tätigkeitsgebiet ein hohes Spezialwissen erlangt haben.

Mit der Benennung von themenspezifischen Qualitätskriterien und der Identifikation geeigneter Dienstleister möchte das BSI betroffenen Unternehmen eine Hilfestellung bei der Suche und Auswahl geeigneter Dienstleister bieten, um die Unternehmen im Ernstfall von einem eigenen zeitintensiven Rechercheaufwand zu entlasten. Gleichzeitig soll auf diese Weise ein gewisses Qualitätsniveau in der jeweiligen Branche etabliert werden.

Zur Identifikation von qualifizierten Sicherheitsdienstleistern für die Abwehr von DDoS-Angriffen hat das BSI Kriterien[1] veröffentlicht, die betroffene Betreiber Kritischer Infrastrukturen bei der Auswahl von geeigneten Dienstleistern unterstützen sollen.

Die Dienstleister, die anhand der Kriterien mit der Hilfe des in Kapitel 2 beschriebenen Verfahrens gefunden wurden, sind in diesem Dokument im Folgenden aufgelistet. Dazu gehören sowohl die Kontaktdaten in Kapitel 3 als auch die Gegenüberstellung der einzelnen Leistungsmerkmale in Kapitel 5. Die Leistungsmerkmale, welche sowohl die Kriterien beinhalten als auch weitere individuelle Unterschiede der Dienstleister darstellen, werden zuvor in Kapitel 4 genauer beschrieben.

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation.html

2 Verfahren

Um den Betreibern Kritischer Infrastrukturen eine leichtere Übersicht über den Markt der DDoS-Mitigation-Dienstleister zu bieten, wurde, basierend auf den Auswahlkriterien, ein Verfahren zur Identifizierung geeigneter Dienstleister durchgeführt.

Das Verfahren gliedert sich in die folgenden Schritte:

1. Überprüfung der vom Dienstleister bereitgestellten Dokumentation
   Der Dienstleister musste zunächst eine vollständige Dokumentation bereitstellen. Hierzu zählten sowohl Beschreibungen der Produkte und Dienstleistungen, als auch Erläuterungen in Bezug auf die Einhaltung der vom BSI aufgestellten Kriterien. Des Weiteren bestand die Möglichkeit, vorhandene Zertifizierungen von Rechenzentren oder dem Unternehmen selbst mitzuliefern.
2. Durchführung eines Fachinterviews
   In einem mehrstündigen Termin beim BSI musste der Dienstleister anhand fiktiver Szenarien zeigen, dass er in der Lage ist, die Situationen fach- und zielgerichtet zu bedienen. Dabei wurde sowohl auf das allgemeine Vorgehen des Dienstleisters, als auch auf gestellte Fragen und Verarbeitung der erhaltenen Informationen geachtet.

Weiteren interessierten Dienstleistern steht das Verfahren jederzeit offen, sie können sich für Informationen an das Funktionspostfach qdl@bsi.bund.de wenden.

3 Qualifizierte DDoS-Mitigation-Dienstleister

Im Folgenden werden die bisher identifizierten qualifizierten DDoS-Mitigation-Dienstleister mit den entsprechenden Kontaktdaten in alphabetischer Reihenfolge aufgelistet.

3.1 Akamai Technologies GmbH

Homepage	https://www.akamai.com/de/de/about/stop-ddos-attacks.jsp
Kontakt-Telefonnummer	+49 (0) 89 94 00 63 08
Kontakt-E-Mail-Adresse	ddos-assistance@akamai.com

3.2 Amazon Web Services

Homepage	https://www.aws.amazon.com
Kontakt-E-Mail-Adresse	bsi-qdl-ddos-mitigation@amazon.de

3.3 Babiel GmbH

Homepage	https://www.babiel.com
Kontakt-Telefonnummer	+49 (0) 211 179 349 0
Kontakt-E-Mail-Adresse	service@babiel.com

3.4 Cloudflare GmbH

Homepage	https://www.cloudflare.com
Kontakt-Telefonnummer	+49 (0) 89 54197220
Kontakt-E-Mail-Adresse	ddos-schutz@cloudflare.com

3.5 Colt Group

Homepage	Colt DDoS Mitigation Service
Kontakt-Telefonnummer	+49 (0) 174 326 1547
Kontakt-E-Mail-Adresse	Kontaktformular Paul.Gadiot@colt.net

3.6 Corero Network Security

Homepage	https://www.corero.com
Kontakt-Telefonnummer	+49 (0) 800 18 21 222
Kontakt-E-Mail-Adresse	notfall@corero.com

3.7 Deutsche Telekom AG

Homepage	https://globalcarrier.telekom.com/business-areas/internet-content/ddos-defense https://geschaeftskunden.telekom.de/magenta-business-networks/netzwerksicherheit/ddos-protection https://public.t-systems.de/it-tk-portfolio/security/network-security/ddos-protection/abwehr-von-cyber-angriffen-403444
Kontakt-Telefonnummer	IP Transit Anschlüsse: +49 (0) 69 20060 5575 Company Connect und Deutschland LAN Connect IP Anschlüsse: +49 (0) 800 5231323

3.8 EWE

Homepage	https://www.ewe.de/unternehmen/telekommunikation/security/ddos
Kontakt-Telefonnummer	+49 (0) 800 1393835
Kontakt-E-Mail-Adresse	business@ewe.de

3.9 F5 Networks

Homepage	https://f5.com https://www.f5.com/de_de/cloud/products/l3-and-l7-ddos-attack-mitigation https://www.f5.com/de_de/solutions/use-cases/ddos-attack-protection
Kontakt-Telefonnummer	+49 (0) 800 7000 5050 (gebührenfrei) +1 (206) 272-7969 (gebührenpflichtig)
Kontakt-E-Mail-Adresse	F5DistCloudEMEA_Sales@f5.com

3.10 Imperva Inc.

Homepage	https://www.imperva.com
Kontakt-Telefonnummer	+1-866-777-9980 (24/7 verfügbar)
Kontakt-E-Mail-Adresse	https://www.imperva.com/contact-us https://www.imperva.com/under-ddos-attack/

3.11 Inter.link GmbH

Homepage	inter.link
Kontakt-Telefonnummer	+4930577037410
Kontakt-E-Mail-Adresse	hello@inter.link

3.12 Link11

Homepage	https://www.link11.com
Kontakt-Telefonnummer	24/7 DDoS Hotline: +49 (0) 800 0011888
Kontakt-E-Mail-Adresse	sales@link11.com

3.13 M-net Telekommunikations GmbH

Homepage	https://www.m-net.de
Kontakt-Telefonnummer	+49 (0) 800 7239848
Kontakt-E-Mail-Adresse	business@m-net.de

3.14 Myra Security GmbH

Homepage	https://www.myrasecurity.com
Kontakt-Telefonnummer	+49 (0) 89 414141 345
Kontakt-E-Mail-Adresse	info@myrasecurity.com

3.15 NaWas by NBIP

Homepage	https://www.nbip.nl/en/nawas/
Kontakt-Telefonnummer	+31 (0)88 237 86 24
Kontakt-E-Mail-Adresse	bureau@connect.nbip.nl

3.16 Netscout

Homepage	https://www.netscout.com/arbor-ddos
Kontakt-Telefonnummer	+49 (0) 151 2077 3122 +49 (0) 151 1630 4551
Kontakt-E-Mail-Adresse	Karl.Heuser@netscout.com Thomas.Dungs@netscout.com

3.17 noris network AG

Homepage	https://www.noris.de
Kontakt-Telefonnummer	+49 (0) 911 9352 1612
Kontakt-E-Mail-Adresse	udo.kuerzdoerfer@noris.de

3.18 Plus.line AG

Homepage	https://www.plusline.net/
Kontakt-Telefonnummer	+49 (0) 69 758 915-0
Kontakt-E-Mail-Adresse	vertrieb@plusline.net

3.19 Radware GmbH

Homepage	https://www.radware.com
Kontakt-Telefonnummer	+49 (0) 6103 59964 96
Kontakt-E-Mail-Adresse	info_de@radware.com

3.20 Verizon Deutschland GmbH

Homepage	https://www.verizon.com/business/de-de/products/security/network-cloud-security/ddos-shield/
Kontakt-Telefonnummer	+49 (0) 231 9720
Kontakt-E-Mail-Adresse	ddos-help-de@verizon.com

3.21 Vodafone GmbH

Homepage	https://www.vodafone.de
Kontakt-Telefonnummer	+49 (0) 800 444063 3000
Kontakt-E-Mail-Adresse	cloud.hosting@vodafone.com

3.22 Voxility

Homepage	https://www.voxility.com/
Kontakt-Telefonnummer	+49 (0) -69-957-98952
Kontakt-E-Mail-Adresse	contact@voxility.com

3.23 WEDOS GmbH

Homepage	https://wedos.global/
Kontakt-Telefonnummer	
Kontakt-E-Mail-Adresse	business@wedos.de

4 Leistungsmerkmale

Im Folgenden werden die einzelnen vergleichenden Leistungsmerkmale dargestellt. Dabei hat das BSI bei der Qualifizierung von DDoS-Mitigation-Dienstleistern bewusst auf die Bewertung von Bandbreiten verzichtet, da sich sowohl die Angriffsbandbreiten dynamisch entwickeln, als auch die notwendige Schutzkapazität abhängig vom Ziel ist. Bei der Auswahl eines geeigneten Anbieters sollte daher neben den vom BSI aufgeführten Kriterien auch die benötigte und mit dem Anbieter besprochene Mitigationsleistung berücksichtigt werden.

4.1 Dienstangebot

4.1.1 Dienstleistung auch für Nicht-Bestandskunden

Werden die angebotenen Dienstleistungen und Produkte auch Unternehmen zur Verfügung gestellt, welche keine weiteren Leistungen des qualifizierten Dienstleisters (zum Beispiel Internet-Leitung) beziehen?

4.1.2 24x7 Erreichbarkeit

Ist der DDoS-Mitigation-Dienstleister rund um die Uhr bei Angriffen oder Problemen erreichbar?

4.1.3 Dienstleister SPOC (für RIPE- und/oder Provider-Kontakte) oder Unterstützung bei Kontaktaufnahme und Kommunikation

Für die Umleitung des Netzwerkverkehrs vom KRITIS-Unternehmen über den DDoS-Mitigation-Dienstleister müssen je nach Größe des umzuleitenden Netzes verschiedene Voraussetzungen und Absprachen zum Beispiel mit dem Provider des KRITIS-Unternehmens getroffen werden. Hierbei sollte der Dienstleister den Kunden unterstützen können.

4.2 Allgemeines zum Dienstleister

4.2.1 ISO27001-Zertifizierung der RZ-Standorte

Sind die Rechenzentren des DDoS-Mitigation-Dienstleisters ISO27001 zertifiziert?

4.2.2 ISO27001-Zertifizierung der Institution

Besitzt der DDoS-Mitigation-Dienstleister eine ISO27001 Zertifizierung für die Institution?

4.2.3 Räumliche Verteilung der RZ

Falls der DDoS-Mitigation-Dienstleister über mehrere Rechenzentren verfügt, ist es sinnvoll, dass diese in einem ausreichend großen Abstand zueinanderstehen. Nur so kann gewährleistet werden, dass regionale Probleme, zum Beispiel bei der Netzanbindung, nicht alle Standorte betreffen.

Des Weiteren bietet eine großflächige Verteilung der Rechenzentren den Vorteil, dass der Netzverkehr in der Nähe des Ursprungs gefiltert werden kann.

4.2.4 Beschränkung auf RZ in Deutschland / EU möglich

Bietet der DDoS-Mitigation-Dienstleister an, dass umgeleiteter Verkehr ausschließlich in Rechenzentren in Deutschland oder der Europäischen Union (EU) verarbeitet wird?

Der Netzwerkverkehr fließt zumindest im Falle einer Mitigation über die Rechenzentren des DDoS-Mitigation-Dienstleisters. Dabei wird unter Umständen auch die Transportverschlüsselung terminiert, sodass der Dienstleister prinzipiell den gesamten Verkehr inklusive aller Eingaben sehen könnte.

Das deutsche Datenschutzgesetz beziehungsweise die Datenschutzgrundverordnung der EU sehen dabei zahlreiche Pflichten vor, welche mindestens dann gelten, wenn sich die Rechenzentren und somit auch die Daten ausschließlich in Deutschland beziehungsweise der Europäischen Union befinden.

Bei einer Verarbeitung von Daten in Rechenzentren außerhalb der EU muss das Angebot im Einzelfall durch den Auftraggeber auf Konformität zur DSGVO geprüft werden.

4.2.5 Redundante Internet-Anbindung

Verfügen die DDoS-Mitigation-Dienstleister über eine redundante Internet-Anbindung? Die redundante Anbindung ist notwendig, damit auch beim Ausfall einer Anbindung weiterhin eine Erreichbarkeit und ein Schutz der Anwendungen von KRITIS-Unternehmen gewährleistet werden kann.

4.3 Angriff

4.3.1 Verkehrsumleitung mittels DNS / BGP

Im Falle eines Angriffs muss der gesamte Netzwerkverkehr über den DDoS-Mitigation-Dienstleister umgeleitet werden, damit dieser den Verkehr filtern kann. Eine Umleitung kann dabei für größere Netzbereiche über das Border Gateway Protocol oder bei wenigen IP-Adressen über DNS-Einstellungen erfolgen. Dabei unterstützt nicht jeder Dienstleister unbedingt beide Varianten.

4.3.2 Optionale Umleitung im Angriffsfall

Besteht die Umleitung des Netzwerkverkehrs über die Rechenzentren des DDoS-Mitigation-Dienstleisters dauerhaft, also auch zu Zeiten, wo kein DDoS-Angriff stattfindet, oder besteht die Möglichkeit, den Netzwerkverkehr ausschließlich im Angriffsfall umzuleiten?

4.3.3 Mitigation im Angriffsfall automatisch aktiv

Falls ein Angriff erkannt wird, greift der DDoS-Mitigation-Dienstleister automatisiert ein oder muss erst ein manueller Start der Mitigation oder eine Anweisung durch das KRITIS-Unternehmen erfolgen?

4.3.4 Unterstützung von IPv4 / IPv6

Werden Verbindungen über die Protokolle IPv4 und/oder IPv6 unterstützt?

4.3.5 Handling verschlüsselter Verbindungen

Kann der DDoS-Mitigation-Dienstleister mit verschlüsselten Verbindungen (HTTPS) umgehen? Dazu muss zum Beispiel der private Schlüssel zu einem TLS-Zertifikat des KRITIS-Unternehmens bereitgestellt werden können, womit auch die Dateneingabe von Kunden eingesehen werden können.

4.4 Filtermöglichkeiten

4.4.1 DDoS-Filter zum Schutz gängiger Dienste

DDoS-Angriffe erfolgen auf unterschiedliche Arten und haben die verschiedensten Dienste als Ziel. Je nach Dienst ist dabei eine unterschiedliche Handhabung notwendig, sodass der DDoS-Mitigation-Dienstleister für alle gängigen Dienste (Web, E-Mail, VPN, DNS) Filter parat haben sollte.

4.4.2 Filtermöglichkeiten

Die Filterung kann auf Basis verschiedenster Ansätze geschehen. Um dabei möglichst alle Angriffe erfolgreich erkennen und abwehren zu können, sollte der DDoS-Mitigation-Dienstleister in der Lage sein,

eine Filterung auf Protokoll-Ebene, mit der Hilfe verschiedener Techniken, wie zum Beispiel TCP-Flags, Quell- und Ziel-IPs sowie Rate-Limiting oder regulären Ausdrücken, durchzuführen können. Des Weiteren können Filterungen auch auf Layer-7-Ebene möglich sein.

4.4.3 Unterstützung des Kunden beim Erstellen eigener Definitionen

Kann der Kunde eigene Definitionen für die Filterung des Netzwerkverkehrs einbringen? Dazu können zum Beispiel IP-Bereiche gehören, die immer freigeschaltet (Allowlisting) oder welche dauerhaft geblockt werden sollen, zum Beispiel Geo-Blocking. Auch allgemeine Profile des erlaubten Verkehrs anhand regulärer Ausdrücke können durch den DDoS-Mitigation-Dienstleister ermöglicht werden.

4.4.4 Automatische Ableitung der Filter-Definition aus Angriffsmustern

Unterstützt der DDoS-Mitigation-Dienstleister eine Verbesserung seiner Filter durch eine automatische Analyse der Angriffe?

4.4.5 Erkennung menschlicher Benutzer / Captcha-Einsatz

Angriffe erfolgen zumeist durch Botnetze und sind dabei automatisiert. Bei der Filterung gegen diese Angriffe ist es potentiell möglich, dass auch normalen Benutzern der Zugang zur Seite verwehrt wird.

Bei diesem Leistungsmerkmal wird abgefragt, ob der Dienstleister die Option bietet, gesperrten Benutzern ein Captcha anzuzeigen, sodass sie durch das Lösen der Aufgabe nachweisen können, dass es sich bei ihnen um reguläre menschliche Benutzer handelt.

4.4.6 Benutzer-Plattform

Die Bereitstellung von Informationen durch den DDoS-Mitigation-Dienstleister geschieht für die Kunden häufig durch eine Benutzer-Plattform. Diese kann auf der einen Seite rein passiv sein und lediglich Statistiken bereitstellen. Auf der anderen Seite besteht aber auch oftmals die Möglichkeit für den Kunden, eigene Definitionen zur Filterung des Netzwerkverkehrs einzubringen.

Des Weiteren wird bei diesem Leistungsmerkmal abgefragt, wie der Zugang zur Plattform gesichert ist (TLS-geschützt, 2-Faktor-Authentifizierung) und ob Rollen/Rechte-Konzepte vorgesehen sind, sodass nicht jeder Mitarbeiter des KRITIS-Unternehmen, welcher Zugang zur Benutzer-Plattform erhalten soll, Zugriff auf alle Funktionsmöglichkeiten erhalten muss.

5 Gegenüberstellung der Leistungsmerkmale der einzelnen DDoS-Mitigation-Dienstleister

Die folgende Tabelle liefert eine grobe Gegenüberstellung einzelner Leistungsmerkmale der DDoS-Mitigation-Dienstleister und soll einen ersten Ansatzpunkt für die Auswahl eines geeigneten Dienstleisters darstellen. Genauere Informationen können nur im Gespräch mit potentiell geeigneten Kandidaten erörtert werden.

Leistungsmerkmale	Akamai Technologies GmbH	Amazon Web Services	Babiel GmbH	Cloudflare GmbH	Corero Network Security	Deutsche Telekom AG	EWE	F5 Networks	Imperva In	Inter.link	Link11	Colt Group	M-net Telekommunikations GmbH	Myra Security GmbH	NaWas by NBIP	Netscout	noris network AG	Plus.line AG	Radware GmbH	Verizon Deutschland GmbH	Vodafone GmbH	Voxility	WEDOS GmbH
4.1 Dienstangebot																							
4.1.1 Dienstleistung auch für Nicht-Bestandskunden	+	+[2]	+	+	+	+	-	+	+[3]	+	+	+[4]	-	+	+	+	-	+	+	+	-	-	+[5]
4.1.2 24x7 Erreichbarkeit	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

[2] Die DDoS-Mitigation ist für Dienste ausgelegt, die in AWS laufen. Für einige Dienste ist es jedoch möglich, AWS als „Frontend“ zu verwenden und eine DDoS-Mitigation auf Layer 3 und 4 zu ermöglichen

[3] Ja, wenn Kunde über einen Reseller angebunden ist. Ansonsten ca. 24 Stunden für die Einrichtung eines Cross-connect.

[4] Notfallaufnahme neuer Kunden kann 12 bis 24 Stunden dauern; regulär bis zu 30 Tage

[5] Neue Kunden können sich einen Account anlegen und eigene Filter anlegen

Leistungsmerkmale	Akamai Technologies GmbH	Amazon Web Services	Babiel GmbH	Cloudflare GmbH	Corero Network Security	Deutsche Telekom AG	EWE	F5 Networks	Imperva In	Inter.link	Link11	Colt Group	M-net Telekommunikations GmbH	Myra Security GmbH	NaWas by NBIP	Netscout	noris network AG	Plus.line AG	Radware GmbH	Verizon Deutschland GmbH	Vodafone GmbH	Voxility	WEDOS GmbH
4.1.3 Dienstleister SPOC (für RIPE- und/oder Provider-Kontakte) oder Unterstützung bei Kontaktaufnahme und Kommunikation	+	+	+	+	– [6]	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–	+	–
4.2 Allgemeines zum Dienstleister																							
4.2.1 ISO27001-Zertifizierung der RZ-Standorte	+	+	+	+	– [7]	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
4.2.2 ISO27001-Zertifizierung der Institution	+	+	+	+	– [7]	+	+	+	+	–	+	+	–	+	–	–	+	+	+	– [8]	+	–	+ [9]
4.2.3 Räumliche Verteilung der RZ	+	+	+	+	– [7]	+	+	+	+	+	+	+	+	+	+ [10]	+	+	+	+	+	+	+	+

[6] Kriterium ist nicht relevant, da Corero Network Security ausschließlich eine Appliance anbietet, welche im Rechenzentrum des Kunden eingebunden und betrieben werden muss.
[7] Kriterium ist nicht relevant, da Corero Network Security ausschließlich eine Appliance anbietet, welche im Rechenzentrum des Kunden eingebunden und betrieben werden muss. Die Angaben zum Rechenzentrum sowie der Anbindung entsprechen somit den vorhandenen Kriterien im Rechenzentrum des Kunden. Auch muss dadurch keine Verkehrsumleitung in andere Rechenzentren erfolgen.
[8] In Erstellung.
[9] Nicht für alle Rechenzentren weltweit
[10] Aktuell nur Rechenzentren in den Niederlanden.

Leistungsmerkmale	Akamai Technologies GmbH	Amazon Web Services	Babiel GmbH	Cloudflare GmbH	Corero Network Security	Deutsche Telekom AG	EWE	F5 Networks	Imperva In	Inter.link	Link11	Colt Group	M-net Telekommunikations GmbH	Myra Security GmbH	NaWas by NBIP	Netscout	noris network AG	Plus.line AG	Radware GmbH	Verizon Deutschland GmbH	Vodafone GmbH	Voxility	WEDOS GmbH
4.2.4 Beschränkung auf RZ in Deutschland / EU möglich																							
Deutschland	–	+[11]	+	+[12]	–[7]	+	+	–	+	+	+	+	+	+	–	+	+[13]	+	+	–	+	–	+
EU	+	+[11]	+	+[12]	–[7]	+	+	+	+[14]	+	+	+	+	+	+	+	+[13]	+	+	+	+	–	+
4.2.5 Redundante Internet-Anbindung	+	+	+	+	–[7]	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
4.3 Angriff																							
4.3.1 Verkehrsumleitung mittels DNS / BGP																							
DNS	+	+	+	+	–[7]	+	–	+	+	–	+	+	–	+	–	+	–	+	+	–	–	–	+
BGP	+	+[11]	+	+	–[7]	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

[11] Eine Annoncierung des Kundennetzes per BGP durch AWS zum Ziel der Mitigation ist nicht vorgesehen. Der Kunde kann jedoch eigene IPs für Dienste in AWS nutzen, die dann auch von AWS annonciert und von der DDoS-Mitigation geschützt sind

[12] Nur im Enterprise-Tarif

[13] Bis 40 Gbit/s, darüber hinaus wird auf Kundenwunsch ein internationales Partnerunternehmen mit Rechenzentren auch außerhalb der EU eingebunden.

[14] im Angriffsfall weltweite Mitigation

Leistungsmerkmale	Akamai Technologies GmbH	Amazon Web Services	Babiel GmbH	Cloudflare GmbH	Corero Network Security	Deutsche Telekom AG	EWE	F5 Networks	Imperva In	Inter.link	Link11	Colt Group	M-net Telekommunikations GmbH	Myra Security GmbH	NaWas by NBIP	Netscout	noris network AG	Plus.line AG	Radware GmbH	Verizon Deutschland GmbH	Vodafone GmbH	Voxility	WEDOS GmbH
4.3.2 Optionale Umleitung im Angriffsfall	+	-	+	+[15]	+	+	+	+	+	+	+	+	+	+	+	+	-	+	+	+	+	+	+
4.3.3 Mitigation im Angriffsfall automatisch aktiv	+	+	+	+	+	+[16]	+	+	+	+	+	+	+	+	-	+	+	+	+	+	+	+	+
4.3.4 Unterstützung von IPv4 / IPv6																							
IPv4	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
IPv6	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-[16]	+
4.3.5 Handling verschlüsselter Verbindungen [17]	+	+	+	+	-	+	-	+	+	-	+	+	-	+	-	+	-[18]	+	+	-	-	+	+
4.4 Filtermöglichkeiten																							

[15] Per BGP
[16] Nur im Premium Tarif
[17] Verschlüsselte Verbindungen können Klartextbestandteile enthalten, die prinzipiell von allen Anbietern ausgewertet zur DDoS-Mitigation genutzt werden können.
[18] Optional durch Appliance möglich.

Leistungsmerkmale	Akamai Technologies GmbH	Amazon Web Services	Babiel GmbH	Cloudflare GmbH	Corero Network Security	Deutsche Telekom AG	EWE	F5 Networks	Imperva In	Inter.link	Link11	Colt Group	M-net Telekommunikations GmbH	Myra Security GmbH	NaWas by NBIP	Netscout	noris network AG	Plus.line AG	Radware GmbH	Verizon Deutschland GmbH	Vodafone GmbH	Voxility	WEDOS GmbH
4.4.1 DDoS-Filter zum Schutz gängiger Dienste																							
Web	+	+[2]	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–[18]	+	+	+	+	+	+
E-Mail	+	+[2]	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–[18]	+	+	+	+	+	–
VPN	+	+[2]	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–[18]	+	+	+	+	–[18]	–[19]
DNS	+	+[2]	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–[18]	+	+	+	+	+	–[20]
4.4.2 Filtermöglichkeiten																							
Layer 7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–[18]	+	+	+	+	+	+
Protokoll	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–[18]	+	+	+	+	+	+
TCP-Flags	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Quell- und Ziel-IP	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

[19] Nur Web-basierte VPN
[20] Es wird Anycast DNS angeboten, jedoch keine speziellen DNS-Filter

Leistungsmerkmale	Akamai Technologies GmbH	Amazon Web Services	Babiel GmbH	Cloudflare GmbH	Corero Network Security	Deutsche Telekom AG	EWE	F5 Networks	Imperva In	Inter.link	Link11	Colt Group	M-net Telekommunikations GmbH	Myra Security GmbH	NaWas by NBIP	Netscout	noris network AG	Plus.line AG	Radware GmbH	Verizon Deutschland GmbH	Vodafone GmbH	Voxility	WEDOS GmbH
Rate-Limiting	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Reguläre Ausdrücke	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
4.4.3 Unterstützung des Kunden beim Erstellen eigener Definitionen																							
Zulässige oder spezielle IP-Bereiche	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	– [18]	+
Zulässige oder spezielle Regionen (GEO-IP)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	– [18]	+
Profile des erlaubten Verkehrs	+	+ [21]	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	– [18]	+
4.4.4 Automatische Ableitung der Filter-Definition aus Angriffsmustern	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

[21] Definitionen auf Layer 3 und 4 nur im Rahmen des Premium Tarifs

Leistungsmerkmale	Akamai Technologies GmbH	Amazon Web Services	Babiel GmbH	Cloudflare GmbH	Corero Network Security	Deutsche Telekom AG	EWE	F5 Networks	Imperva In	Inter.link	Link11	Colt Group	M-net Telekommunikations GmbH	Myra Security GmbH	NaWas by NBIP	Netscout	noris network AG	Plus.line AG	Radware GmbH	Verizon Deutschland GmbH	Vodafone GmbH	Voxility	WEDOS GmbH
4.4.5 Erkennung menschlicher Benutzer / Captcha-Einsatz																							
Benutzer	+	+	+	+	-	+	-	+	+	+	+	-	-	+	-	-	+	+	+	-	+	+	+
Captcha-Einsatz	+	+	+	+	-	+	-	+	+	-	+	-	-	+[22]	-[23]	-	+	+	-	-	-	-[24]	+
4.4.6 Benutzer-Plattform																							
TLS-geschützt	+	+	+[25]	+	+	+	+	+	+	+	+	+	+	+	-[26]	+	+	+	+	+	+	+	+
2-Faktor-Authentifizierung	+	+	+[25]	+	-[27]	+	+	+	+	+	+	-	-	+	-[26]	+	-	+	+	+	-	-	+
Verschiedene Rollen/Rechte-	+	+	+[25]	+	+	-	+	+	+	+	+	+	-	+	-[26]	+	-	+	+	+	+	+	+

[22] Auf Wunsch möglich.
[23] Capcha nur bei unverschlüsselten Verbindungen.
[24] Es wird eine Authentifizierung über Cookies vorgenommen
[25] Kein Portal zur Konfiguration, da managed Service. Ticket-System verfügbar.
[26] Kein Portal für Kunden verfügbar.
[27] Im Laufe des Jahres verfügbar.

Leistungsmerkmale	Akamai Technologies GmbH	Amazon Web Services	Babiel GmbH	Cloudflare GmbH	Corero Network Security	Deutsche Telekom AG	EWE	F5 Networks	Imperva In	Inter.link	Link11	Colt Group	M-net Telekommunikations GmbH	Myra Security GmbH	NaWas by NBIP	Netscout	noris network AG	Plus.line AG	Radware GmbH	Verizon Deutschland GmbH	Vodafone GmbH	Voxility	WEDOS GmbH
Statistiken	+	+[16]	+[25]	+	+	+	+	+	+	+	+	+	+	+	+[28]	+	+	+	+	+	+	+	+
Möglichkeit zur Eingabe eigener Definitionen	+	+[21]	+[25]	+	+	−[29]	+	+	+	+[30]	+[31]	+[32]	−[29]	+[31]	−	+	−[33]	+	−	+	+[34]	−	+

[28] Statistik-Report wird automatisch per E-Mail verschickt; Plattform existiert nicht.
[29] Einbringung eigener Definitionen über Kunden-Support möglich.
[30] Ab Premium Tarif
[31] Allow- und Denylisting von IP-Adressen und Bereichen, Angabe individueller Fehlerseiten, DNS-Editor, ...
[32] Definitionen können über das Portal beantragt werden und werden händisch durch das SOC umgesetzt.
[33] Optional durch Appliance möglich.
[34] Allowlisting von IP-Adressen.